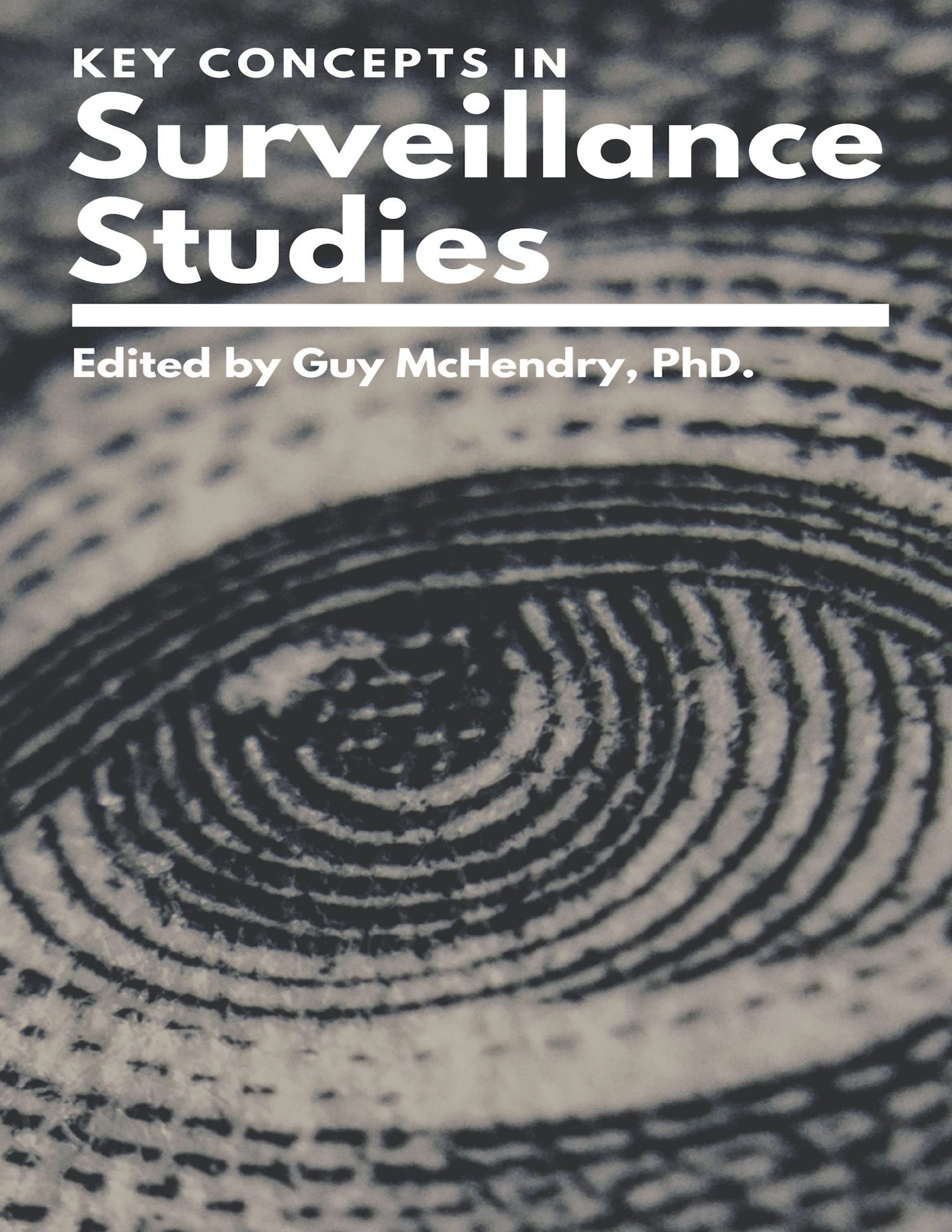


KEY CONCEPTS IN

Surveillance Studies

Edited by Guy McHendry, PhD.

Key Concepts in Surveillance Studies

GUY MCHENDRY, PH.D.

•

Contents

Dedication

For all the students who have given so much of their energy and intellect to our conversations about surveillance over the years; know you teach me as much as I teach you.

Forward

Years ago, when I first began teaching COM 174 From Big Brother to Big Data: Surveillance Culture at Creighton University, I had no idea how students would respond to the course. They have been nothing short of amazing. The course has been through several iterations since I began with a framework shared by my friend and colleague Sean Lawson at the University of Utah for a similar class. With each new semester, the course material becomes more complex. Too often, we find ourselves working through complex webs of terminology. In response to that trend, I began to think about ways to make critical concepts more available in the class. Inspired by folks I've encountered who work on collaborative resources authored by students, I decided that my students and I would write a glossary of key terms in surveillance studies.

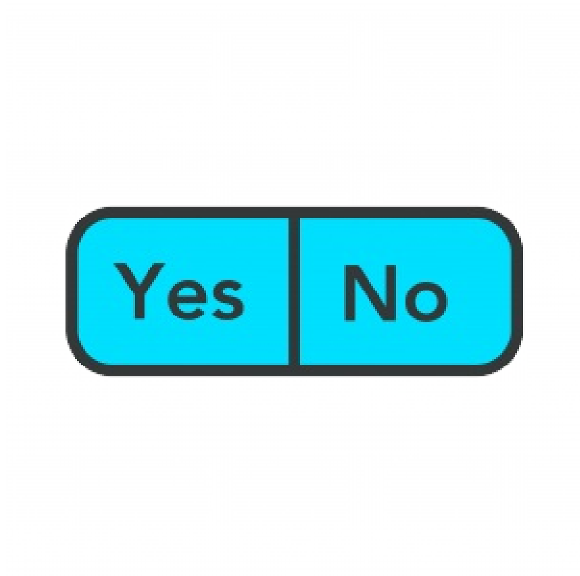
I developed a list of almost 200 terms that we discuss in the course. From that list, I selected the 50 I viewed as most important. I asked students to choose a term, offer a concise definition of the concept that makes its connection to surveillance studies clear, and to provide a clear example of the concept. Students jumped in, researching, writing, and revising. The entries in this glossary represent the work of students who voluntarily agreed to share their work publicly. This edition contains 26 entries from students. I plan to continue the project in future semesters, adding concepts along the way. I have left this project so appreciative of the work students do and their willingness to experiment with me along the way.

Call for Contributions

I would love to collaborate with other instructors who teach on the topic of surveillance and security. If you would like to use this assignment in your classes and help grow this project, please contact me at gmchendry@creighton.edu.

1. **Affordances**

Bethany Baumgartner



Affordances are ways that a user is able to use, manipulate, and change technology available. Developers of technology have intended uses, however, consumers work around the original parameters and constraints to do other things. For example, sociologist Ian Hutchby describes communicative affordances as “possibilities for action that emerge from […] given technological forms” (Bucher & Helmond, 2018, p. 7). Therefore, they’re the alternative functions of a technology that the designer didn’t think possible or intend for.

Affordances are a form of surveillance that allows people to expand the influence and reach of technology. It can therefore change people’s behavior both as consumers–how they interact online–and as developers–how they form the layout of their technology and what tools they make available to consumers. An example of affordances can be found on the social networking site Twitter; by design users had a limited number if characters available but were permitted to attach photos and reply to tweets. As an effect, users manipulated the function to attach pictures by taking screenshots of larger text and attaching it to the original tweets. They also commented continuously, forming threads that allowed them to say everything they wanted to. Twitter changed its design by allowing 280 characters on a tweet, compared to the original 140 (Larson, 2017). This affordance is a way users worked around the original constraints to achieve what they wanted. For consumers, "imagination is the capacity to break with the ordinary, the given…to challenge the controlled" (Lin, 2017, p.2). Consumers have power when they use affordances.

References

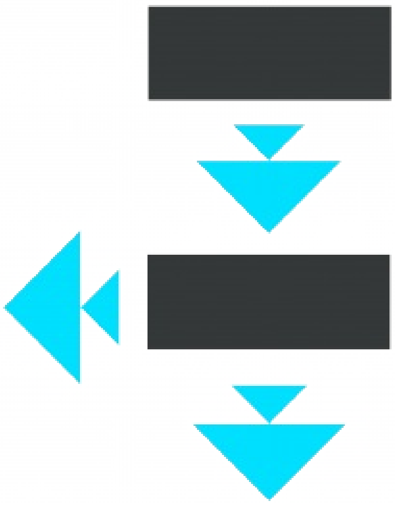
Bucher, T., & Helmond, A. (2018). The affordance of social media platforms. In J. Burges, A. Marwick, T. Poell (Eds), The SAGE handbook of social media. http://sk.sagepub.com/reference/download/the-sage-handbook-of-social-media/i1867.pdf

Larson, S. (2017, November 7). Welcome to a world with 280-character tweets. CNN. Retrieved from https://money.cnn.com/2017/11/07/technology/twitter-280-character-limit/.

Lin, Y.-W. (2017). A reflective commentary of teaching critical thinking of privacy and surveillance in UK higher education. Big Data & Society, 1-6. https://doi.org/10.1177/2053951717694054

2. Algorithmic Surveillance

Frankie Frericks



Algorithmic surveillance is surveillance that is performed by technology with the use of algorithms. Algorithms are any program used to do a computation from an input to get some sort of an output (Watcher-Boettcher, 2017). These algorithms are then used in various technologies to make clarifications and educated guesses on human beings. It is a form of automated decision-making. Boyd, Levy, Marwick (2014) describe algorithmic surveillance as "Along with information about who you know, technical mechanisms that underlie the "big data" phenomenon—like predictive analytics and recommendation systems—make imputations about who you are like, based on your practices and preferences" (p. 54). These systems are surveillance because they make judgments about people by monitoring their current and past behavior. Murphy (2016) states, “it is also now clear that the algorithmic processing of mass data sets plays an essential role in the modern government surveillance apparatus” (p.1). The information computed by algorithms play a huge role in modern surveillance.

An example of the use of algorithmic surveillance is COMPAS. COMPAS stands for Correctional Offender Management Profiling for Alternative Sanctions. This app uses algorithms to determine how dangerous, and how much of a threat, criminals are on a scale of 1-10. What the COMPAS app takes into account while computing its’ ratings of criminals is hard to know, because the designers of the app usually don’t share these (Wachter-Boettcher, 2017). There are many reasons algorithmic surveillance can help us take a critical approach to surveillance. First of all, algorithmic surveillance can be extremely biased. According to Watcher-Boettcher “COMPAS might be a particularly problematic example- it can directly affect how long a convicted player spends in jail, after all. But it’s far from alone. Because, no matter how much tech companies talk about algorithms like their advanced math, they always reflect the values of their creators: the programmers and product teams working in tech. And as we’ve seen time and again, the values that tech culture holds aren’t neutral” (p. 121). This helps explain why many people associated with the criminal justice system see COMPAS as racially biased. The creators of COMPAS design the algorithms in a way that support their existing thinking on criminality. If their views include racial bias, then COMPAS will show racial bias as well.

References

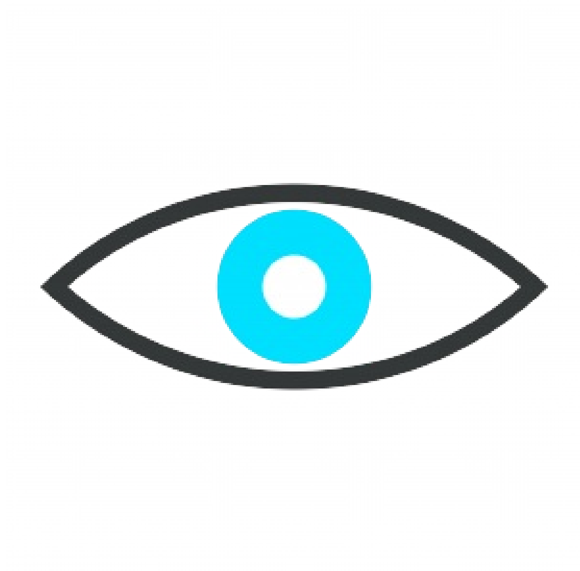
Boyd, D., Levy, K., Marwick, A. (2014). The networked nature of algorithmic discrimination. Open Technology Institute. Retrieved from https://www.danah.org/papers/2014/DataDiscrimination.pdf

Murphy, M. H. (2016). Algorithmic surveillance: True negatives. Tech Law for Everyone. Retrieved from https://www.scl.org/articles/3717-algorithmic-surveillance-true-negatives

Wachter-Boettcher, S. (2018). Technically wrong: Sexist apps, biased algorithms, and other threats of toxic tech. New York, NY: W. W. Norton & Company.

3. **Biometrics**

Nathaniel Finck



Biometric technology is the use of human characteristics to identify individuals and is a form of surveillance. The word biometric is derived from the Greek words bio (which means life) and metric (which means to measure). Common forms of biometrics are fingerprint scanners and face identification. They can be used in workplaces to ensure security of buildings by only allowing access to certain people. Other forms of biometrics include hand geometry, iris recognition, and DNA. Biometrics can also include behavioral patterns such as signatures or voice recognition (Agarwal, n.d.). Biometric peer surveillance has been around for a very long time, as people have always been able to recognize other individuals by facial features, body characteristics, voice and more. Around 500 BC, fingerprints were taken onto clay tablets during

Babylonian business transactions, and the Chinese recorded footprints to distinguish children in as early as the 14th century. This has all led to the immense field of biometric technology today (Nadeau, 2012).
Biometric technology is becoming much more popular with the rise of surveillance and artificial intelligence. As cameras become more advanced, the use of biometrics will increase significantly. "Particularly over the last several years, with the advent of facial recognition that can scan hours and hours of photos, video footage, and even live feeds, the real potential of biometric technologies in this field has begun to emerge." (The Ongoing Ascent, 2018, para. 1). This technology has turned into a threat to our privacy as well as an aid in various areas of surveillance. Perala (2018) suggests that facial recognition can and will be used in the military, as the U.S. Army Research Laboratory has developed a way to convert thermal images to recognizable facial portraits using artificial intelligence and machine learning technologies. Another example of facial recognition is in stores. When a customer walks into a store, cameras can recognize their face and connect it to their profile. From there, employees will be able to know exactly what the customer wants and can personally recommend products that they might be interested in. The U.S. Government is already in the process of building the world's largest cache of facial recognition data. Their goal is to recognize any and every face in the country. Current laws do not protect Americans from having webcams scan their facial data (Chayka, 2014). Chayka explains, "The creation of such a database would mean that anyone could be tracked wherever his or her face appears, whether it's on a city street or in a mall." We should be critical when discussing biometric surveillance because they pose clear dangers to our privacy.

References

Agarwal, T. (n.d.) Biometric sensors – Types and its working. Elprocus: Electronics, Projects, Focus. Retrieved from https://www.elprocus.com/different-types-biometric-sensors/

Chayka, K. (2014) Biometric surveillance means someone is always watching. Newsweek Magazine. Retrieved from https://www.newsweek.com/2014/04/25/biometric-surveillance-means-someone-always-watching-248161.html

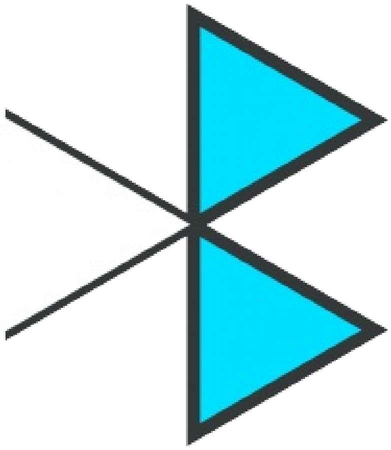
Perala, A. (2018). Army researchers' algorithm tech converts thermal images to conventional portraits. Find Biometrics: Global Identity Management. Retrieved from https://findbiometrics.com/army-researchers-algorithm-tech-thermal-images-conventional-portraits-504185/

The ongoing ascent of biometric surveillance. (2018). Find Biometrics: Global Identity Management. Retrieved from https://findbiometrics.com/brief-biometric-surveillance-504230/

Nadeau, L. K. (2012) Tracing the history of biometrics. Government Technology. Retrieved from http://www.govtech.com/Tracing-the-History-of-Biometrics.html

4. **Bluetooth**

Michela Tarantolo



Bluetooth technology allows users to connect to other devices, share data, and transfer information wirelessly from one device to another. Bluetooth has many great qualities, such as its simplicity, which makes it easy to use and convenience. It allows users to connect quickly with their headphones, speakers, and other various devices nearby. It relates to surveillance studies because Bluetooth can easily track one's location and our information can be at risk (Gilliom & Monahan, 2013). Since a user has the option of allowing connections, we can choose to open ourselves to this form of surveillance. Enabling Bluetooth can put a user at risk, "Be careful with your Bluetooth: 'bluesnarfing' hackers can access a Bluetoother's address book, email, and call history…" (Gilliom & Monahan, p.15) Bluesnarfing makes it possible to become vulnerable towards hackers as they can completely control your phone. Haataja et al. (2013) explains, “Because Bluetooth is a wireless communication system, there is always a possibility that the transmission could be deliberately jammed or intercepted, or that false or modified information could be passed to the piconet devices” (p. 2). Bluetooth is a technology which enables lots of forms of surveillance.

An example of Bluetooth technology and surveillance is Bluetooth scanners. Researchers found that these scanners “covertly tracked [people] without their consent in a technology experiment which has installed scanners at secret locations in offices, campuses, streets and pubs to pinpoint people’s whereabouts.” (Lewis, 2008, para. 1). These scanners are designed to become a new way to target advertisements towards customers at certain times, such as when they enter a specific store. This tactic can have extremely positive results and could even be sustainable as it would eliminate flyers, catalogs, and coupons.

References

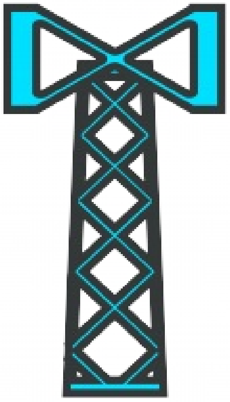
Gilliom, J., & Monahan, T. (2013). SuperVision: An introduction to the surveillance society. Chicago, IL: The University of Chicago Press.

Haataja, K., Hyppönen, K., Pasanen, S., and Toivanen, P. (2013). Bluetooth security attacks: Comparative analysis, attacks, and countermeasures. New York, NY: Springer

Heidelberg, L. P. (2008, July 20). Bluetooth is watching: Secret study gives Bath a flavour of Big Brother. The Guardian. Retrieved from https://www.theguardian.com/uk/2008/jul/21/civilliberties.privacy.

5. **Cell Towers**

Emma Thurmond



A cell tower is a raised structure, containing transmitters and receivers that create a cellular network. Cell towers cover “large service areas [that] are divided into honeycomb-shaped segments or ‘cells’—each of which is equipped with a low-power transmitter or base station which can receive and radiate messages within its parameters” (Owsley, 2013, p.3). When users want to send a message on their phone it sends out a signal and the nearest cell tower picks it up. Then, the message is sent on through a network of cell towers to deliver the message. Cell towers are able to locate a cell phone, this function is called cell tower triangulation (Owsley, 2013).

Cell towers are related to surveillance studies because this technology has the ability to pinpoint your location using your cell phone. Your location is being surveilled and data is being collected about you. For example, cell towers create “data dumps created from cell towers and POIs [Points of Interest] extracted from a popular social network service, Weibo” (Wang et al., 2016, p. 327). Weibo is a “popular Chinese social network web site...” (Wang et al., p. 328). Wang et al. used this data to identify which restaurants were most popular in the city of Guangzhou. They used cell tower data dumps to map where cell phones were and compared the data to the location of restaurants in the city. This example shows how the data collected from cell towers can promote surveillance. However, this function is not unique to Weibo and many other services make use of cell location data. The data collected by towers could later on be used to target you with advertisements to restaurants in your area or attractions that are near where you spend a lot of your time.

Cell towers are an important and powerful form of technology used for surveillance. Cell towers are a threat to users’ privacy. The “Supreme Court has found the right to privacy rooted within the Constitution based on various amendments. In the modern era, with rapid advances in technology, threat to privacy abound, including new surveillance methods by law enforcement” (Owsley, 2013, p.1). It is essential to understand the power of cell tower surveillance.

References

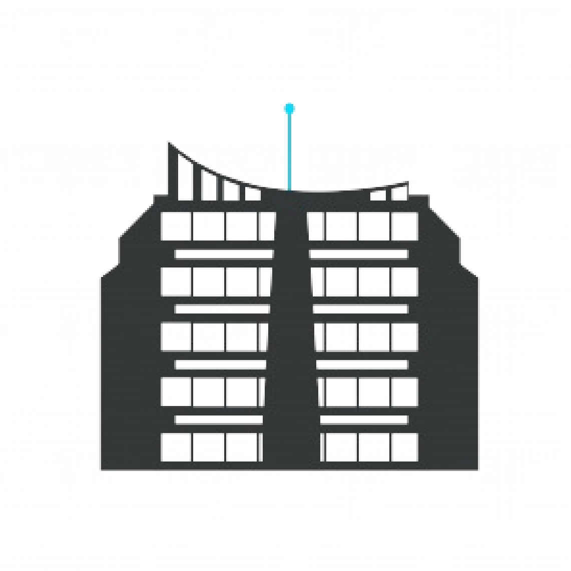
Owsley, Brian L. (2013). The Fourth Amendment implications of the government’s use of cell tower dumps in its electronic surveillance. University of Pennsylvania Journal of Constitutional Law, 16(1), 1-48.

Wang, R., Chow, C.-Y., Lyu, Y., Lee, V., Nutanong, S., Li, Y., & Yuan, M. (2016). Exploring cell tower data dumps for supervised learning-based point-of-interest prediction (industrial paper). GeoInformatica, 20(2), 327–349.

https://link.springer.com/content/pdf/10.1007%2Fs10707-015-0237-7.pdf

6. **Corporate Surveillance**

Jiarong Chen



Corporate surveillance refers to a host of efforts by corporations to collect and use data in a variety of ways to enhance their profitability. This includes surveillance of employees, customers, and competitors. “In recent years, a wide range of companies have started to monitor, track and follow people in virtually every aspect of their lives” (Christl, 2017, para. 1). Big corporates like Amazon and Target use our personal data and information to increase profits. These companies use surveillance techniques to target customers. In other words, Corporate Surveillance is a power that is not shared equally between customers and corporations. Corporate surveillance and surveillance studies are well connected. Corporations use different surveillance techniques, including data mining, tracking customer internet use with cookies , and loyalty cards.

As more and more advanced surveillance technologies come out, it is harder for us to realize how corporate surveillance infiltrates our daily lives. Things we do not pay attention to turn our data into profits. For example, customer loyalty cards may provide discounts, but they can also be used to monitor customers. Customer loyalty cards can automatically record customers' buying habits, their location, and what methods they pay so that a corporation can target individuals with advertisements (Gilliom & Monahan, 2013). In surveillance studies, the concept of corporate surveillance helps us understand the fact that surveillance culture is a key part of the function of our economy.

References

Christl, W. (2017). Corporate surveillance in everyday life. Cracked Labs: Institute for Digital Culture. Retrieved from http://crackedlabs.org/en/corporate-surveillance.

Gilliom, J., & Monahan, T. (2013). SuperVision: An introduction to the surveillance society. Chicago, IL: The University of Chicago Press.

7. Cyberstalking

Morgan Szarka

Cyberstalking is one of the more dangerous and negative examples of surveillance. “Cyberstalking is the repeated unwanted relational pursuit of an individual through communication technologies, such as computers, tablets, and smart phones” (Tokunaga & Aune, 2017, p. 1453). Cyberstalking is a prime example of peer surveillance but to a violent extent. According to Ellison and Akdeniz (1998), “It may involve electronic sabotage, in the form of sending the victim hundreds or thousands of junk e-mail messages (the activity known as ‘spamming’) or sending computer viruses” (pp. 30-31). They also argue cyberstalking includes indirect forms of harassment such as a stalker impersonating his or her victim online and sending abusive e-mails or fraudulent spams under their name (Ellison & Akdeniz).

With the increase in electronic communication and surveillance systems, cyberstalking has become much more prevalent. It is easy for someone to hide behind a screen and harass someone than it is to harass someone face-to-face. Melander (2010) discovered that many stalking behaviors in college relationships are tied to Internet use. Moreover, having or pursuing relationships through technology makes cyberstalking convenient and even enticing for perpetrators (Melander). Social media is a huge enabler for this kind of crime. Anybody can make a fake profile on Facebook or Instagram and use it to stalk someone else.

Furthermore, it is difficult for law enforcement define and investigate cyberstalking. Bocij and McFarlane (2002) explain, “the challenge faced by law enforcement, clinicians, researchers and victims is that of producing a definition of cyberstalking that can be used to formulate legislation, direct research, inform treatment and protect victims” (p. 32). Technology is so complex and has many different channels that allow for violent/dangerous surveillance like cyberstalking.

Cynthia Armistead’s case offers an example of cyberstalking. She received thousands of offensive telephone calls after a stalker posted a fake advertisement on a Usenet discussion group which offered services as a prostitute with her address and phone number attached. She received humiliating and vulgar phone calls and texts for weeks. (Ellison and Akdeniz 1998). Not only is this an annoyance, it can also lead to more serious effects such as anxiety and fear.

References

Bocij, P., & McFarlane, L. (2002). Online harassment: Towards a definition of cyberstalking. Prison Service Journal 139, 31-38. Retrieved from https://www.researchgate.net/profile/Paul_Bocij/publication/284807 harassment-Towards-a-definition-of-cyberstalking.pdf?origin=publication_detail

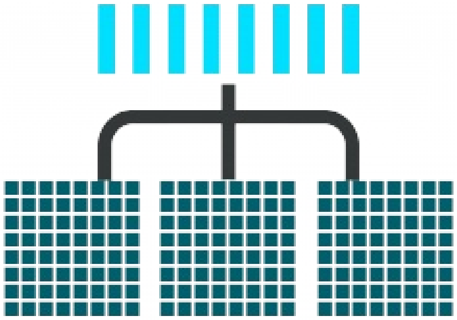
Ellison, L., & Akdeniz, Y. (1998). Cyber-stalking: The regulation of harassment on the internet. Criminal Law Review, 29-48.

Melander, L. A. (2010). College students' perceptions of intimate partner cyber harassment. Cyberpsychology, Behavior, and Social Networking, 13, 263-268. doi:10.1089/cyber.2009.0221

Tokunaga, R., & Aune, K. (2017). Online harassment: Towards a definition of cyberstalking. Journal of Interpersonal Violence, 32(10), 1451-1475. doi: 10.1177/0886260515589564

8. **Data Aggregation & Data Mining**

Alex Littleton



Data aggregation is the act of linking data with other users to analyze trends and track user behavior. Data mining refers to extracting data from user activities to create a profile of individual people (Gilliom and Monahan, 2013). As with all methods of surveillance, data aggregation and mining can have some serious implications surrounding privacy. Data aggregation and mining deal directly with obtaining user data through methods of surveillance through monitoring credit card transactions, internet search history, social media use, etc. and linking that data with other users to track their behavior. This could result in an organization or company having power over others, particularly when companies obtain individuals data in order to try and sell products and services to them (Gilliom and Monahan).

Data aggregation and mining is present in our everyday lives. For example, the tech company Kinsia makes smart-thermometers that sync up to users' smartphones and track fevers and symptoms. This product has become popular to parents with young children. Kinsia aggregated the data it collected from users and sold it Clorox. Clorox then targeted ZIP codes around the country with an increase in fevers with advertisement for products such as disinfecting spray or wipes (Maheshwari, 2018). Another example of data aggregation and mining would include Acxiom. Acxiom is a data aggregator that has data on each and every one of us such as our retail interests, credit score, clothing sizes, income, race, and even our address (Gilliom and Monahan, 2013). Acxiom sells this data to interested companies which then target us as potential consumers with advertisements.

Al-Saggaf and Islam (2015) explore the potential danger that data mining could have regarding social networking sites. Data mining algorithms can derive private information about individuals from social networking sites (Al-Saggaf and Islam). However, data aggregation and mining can prove to be very useful as well. For example, in the smart agriculture industry, data aggregation is being used to make farms more cost-effective which benefits consumers and farmers. The smart agriculture industry along with many other industries could benefit immensely in the near future (Smart, 2018). It is important to remember the power data aggregation and mining gives to those who control our data.

References

Al-Saggaf, Y., & Islam, M. (2015). Data mining and privacy of social network sites' users: Implications of the data mining problem. Science

& Engineering Ethics, 21(4), 941-966. https://doi.org/10.1007/s11948-014-9564-6

Gilliom, J., & Monahan, T. (2013). SuperVision: An introduction to the surveillance society. Chicago, IL: University of Chicago Press.

Maheshwari, S. (2018, October 23). This thermometer tells your temperature, then tells firms where to advertise. The New York Times. Retrieved from https://www.nytimes.com/2018/10/23/business/mediafever-advertisements-medicine-clorox.html

Smart agriculture market is likely to register a 13.50% CAGR between 2017 and 2025, projects TMR. (2018, October 23). Digital Journal. Retrieved from http://www.digitaljournal.com/pr/3992890

9. **Democracy**

Ben Engle

Democracy is a governing system in which the power and authority of the state is drawn from the people. Democracy is often a driving force for the implementation of surveillance. Most modern states, including the United States, employ a form of a representative democracy, where citizens vote for representatives to run the government and make legislation, rather than a direct democracy, where the citizens themselves vote on legislation (Kessler, 2005).

Democracy and surveillance share an intrinsic relationship together. Democracy uses surveillance to fulfill its duties to the people, but also can be at the risk of letting exceptionally intrusive surveillance destroy itself (Bigo, 2014). In order for a democracy to satisfy its requirements to provide fair elections, law enforcement, and protection of individual liberties, an infrastructure must exist to collect data. As populations and the addition of civil duties of government grew, “bureaucratic organization [to evolve] as a means of coordinating activities,” (Lyon, 1994, pp.33). The organization required for a democracy to maintain services can also inhibit its role to protect the rights of citizens when, “[security] forms exceptional measures beyond the realm of normal politics and rule of law,” destroying democratic ideals (Bigo, 2014, pp. 277).

An example of this paradox exists in Turkey’s criminal justice system. In an attempt to decrease the usage of confessions and testimonies, the Turkish criminal justice system is pushing to rely on DNA forensics for evidence-based investigations, in addition to creating a national DNA database. This would make investigations simpler and produce more reliable evidence while also increasing the investigation capabilities of the government over people and cause the collection of sensitive personal data (Bahçecik, 2015). People, rather than being safeguarded by government tyranny, are deprived of sensitive and private information and placed under increasing social control by the government.

References

Bahçecik, Şerif O. (2015). The power effects of human rights reforms in Turkey: Enhanced surveillance and depoliticization. Third World Quarterly, 36(6), 1227. doi: 10/1018/01436597.2015.1047204

Bigo, Didier. (2014). Security, surveillance, and democracy. In K. Ball, K. Haggerty, & D. Lyon (Eds). Routledge handbook of surveillance studies (277-284). New York, NY: Routledge.

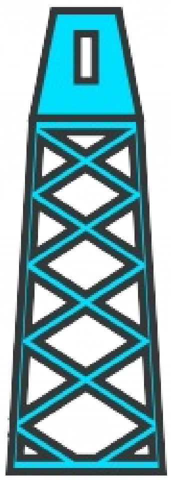
Elements of democracy. (2007). Calabasas, CA: Center for Civic Education.

Kessler, A. S. (2005). Representative versus direct democracy: The role of informational asymmetries. Public Choice, 122(1), 10.

Lyon, D. (1994). Electronic eye: The rise of surveillance society. Minneapolis, MN: University of Minnesota Press.

10. **Disciplinary Society**

Sydney Grad



A disciplinary society is a society where one becomes a docile body due to the presence, or threat of, constant surveillance. Disciplinary society was a term first used by Michel Foucault to describe a condition of surveillance. Doolin (1998) argues that the United States of America resembles a disciplinary society due to the large presence of social media, school security resources, and even hospital surveillance (Doolin, 1998). Foucault himself describes disciplinary societies as “Whereas government is also a function of technology: the government of individuals, the government of souls, the government of the self by the self, the government of families, the government of children, and so on” (Rabinow, 1984, p. 256). In a disciplinary society the subjects/people become docile bodies, who begin to internalize surveillance, and no longer resist. This is often times seen in locations such as schools or factories (Boagrd, 1991).

When used together, these tools become the basis for Foucault's disciplinary society. This society creates a power imbalance, between those executing the surveillance, and those under surveillance. Unlike previous societies, the disciplinary society doesn't use demonstrations of power to scare their subjects into behaving, it is the presence of observation that scares subjects into submission. Lyon (1994) argues that surveillance has taken a larger role in modern capitalistic society. In such cases, disciplinary societies can also relate to surveillance practices such as Fordism and Taylorism. A disciplinary society can also link to other forms of surveillance commonly found in places such as school and work —including cameras, RFID cards, and the more drastic example of the Panopticon.

A specific example of a disciplinary society in modern times is in schools, due to the fact that society sees young children as easily impressionable (Besley, 2002). For example, schools can remotely activating webcams from school issued laptops to monitor; in one instance a student was accused of improper behavior whole at home and was then shown a photograph that had been taken from the laptop (Keizer, 2010). This is life in a disciplinary society because it is the thought that students are being constantly monitored that encourages them to stay on their best behavior at all times, even if they may not be currently monitored.

References

Besley, T. (2002). Social Education and Mental Hygiene: Foucault, Disciplinary Technologies and the Moral Constitution of Youth. Educational Philosophy and Theory, 34(4). doi: 10.1080/0013185022000011835

Bogard, W. (1991). Discipline and Deterrence: Rethinking Foucault on the Question of Power in Contemporary Society. Social Science Journal, 28(3).

Doolin, B. (1998). Information technology as disciplinary technology: Being critical in interpretive research on information systems. Journal of Information Technology, 13 (4).

Foucault, M. (1977). Discipline and Punish. (Alan Sheridan, Trans.). France: Gallimard.

Keizer, G. (2010). Pennsylvania schools spying on students using laptop webcams, claims lawsuit. Computer World. Retrieved from https://www.computerworld.com/article/2521075/windows-pcs/pennsylvania-schools-spying-on-students-using-laptop-webcams–claims- lawsuit.html

Lyon, D. (1994). Electronic eye: The rise of surveillance society. Minneapolis, MN: University of Minnesota Press .

Rabinow, P. (1984). The Foucault reader. New York, NY: Pantheon Books.

11. **Docile Bodies**

Maura Small

Docility occurs when a group of people are so used to being watched continuously that their discipline becomes internalized and they no longer have the capacity to resist. When people enter into this state, they become docile bodies. The group is under constant surveillance. This makes it so others can exert power over them without taking as much action (Corbett, 2010). The more powerful controlling group makes harsh and public examples of those who are caught acting out. This leads to the rest of the group not knowing if or when they could be caught and forces them to watch themselves to avoid the harsh punishments they have seen previously (Urbina, 2016). Surveillance connects to docility and the prospect of docile bodies in many ways. An obvious example includes someone in a place of power watching or surveilling a group (Corbett).

The person in power is doing this to change the group's behavior to meet a certain expectation. (Corbett) Individuals have to watch themselves and be cautious not to break the rules or else they could be punished (Urbina).

An example of docility is the Panopticon prison design. The design includes a central tower for guards (Horne, 2014). The prison cells surround this tower with one-way windows facing in. The windows make it so that the guards could be watching the prisoners at any time (Horgan). This idea was originally developed by a French philosopher Michel Foucault (Horne). The idea was that since the prisoners would never know if they were being observed or not they would avoid doing anything that could lead to punishment (Horgan).

References

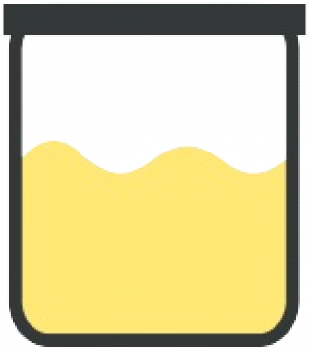
Corbett, M. (n.d.). Docile Bodies. Retrieved from http://sk.sagepub.com/reference/casestudy/n119.xml

Horne, E., & Maly, T. (2014). The inspection house: An impertinent field guide to modern surveillance. Toronto: Coach House Books.

Urbina, K. (2016, February 2). The Many Forms of A Docile Body. Retrieved from https://medium.com/your-philosophy-class/the-many-forms-of-a-docild

12. Drug Testing

Olivia Tidwell



Drug testing is the ability to screen for the presences of both illicit and legal drugs within someone's body (Smith, 2013). In the United States, drug testing became prevalent due to the introduction by the Department of Defense in order to test their military personnel in the 1960s (Smith, 2013). Since then drug testing has been introduced in the workplace due to increased anti-drug attitudes during the 1980s (Smith, 2013). The transportation, energy, and other "safety-sensitive" sectors of the economy rely on drug testing of their workers (Smith, 2013). However, a drug test can be conducted by any employer both upon application and in the duration of one's employment there (McCarty, 2014). Companies can screen for marijuana, cocaine, opiates, amphetamines, tobacco, and other aspects that may hinder job performance and increase company liability

(Smith, 2013). However, drug tests can deter people from obtaining employment and invade on employees' privacy. Drug testing in the workplace is considered a modern application of the philosophy of Henry Ford. Under his employment, Ford would bring evaluators to the employee's homes to inspect for habits of gambling, alcoholism, and other indicators of their morality (Gilliom, 2013). Ford was able to extend the reach of employers into the private lives of his employees, a practice that continues today via corporate drug testing.

Along with its presence in the workplace, drug testing has become a vital aspect of the U.S.'s welfare and entitlement programs. Temporary Assistance for Needy Families (TANF) is a grant program that is funded by the federal government (McCarty, 2014). This money is given to the states to use and implement with their discretion. Some states have implemented drug testing for applicants and recipients of this entitlement (Office of the Assistant Secretary for Policy and Evaluation, 2011). In addition, some states require a personal questionnaire that may result in a drug test by the overseeing agency (CLASP, 2016). Other entitlement programs like the Supplemental Nutrition Assistance Program (SNAP) and federal housing assistance do not have explicit protections for applicants against drug testing; thus their implementation has followed that of TANF (McCarty, 2014). Despite strong political support for welfare drug testing, the system is largely ineffective as the vast majority of welfare recipients are not dependent on illicit drugs. A 2002 study showed that only 4% of welfare recipients are drug depended and only 11% would use drugs recreationally (Walker, 2018). These programs then deny assistance to those who fail such tests and restrict aid to applicants who possess a drug-related felony (McCarty, 2014). Drug testing contributes to the surveillance society because it allows employers to mandate the actions of an employee outside of work hours. Drug testing also creates a system against those who suffer from drug addiction as they will be unable to get or maintain a job due to drug testing and then will be unable to receive the need assistance from the government due to their lack of employment.

References

Hall, R. (2016). Drug testing and public assistance. CLASP: Policy solutions that work for low-income people. Retrieved from: https://www.clasp.org/sites/default/files/publications/2017/04/2016. Drug-Testing-and-Public-Assistance-Brief-FINAL.pdf

Gilliom, J., & Monahan, T. (2013). SuperVision: An introduction to the surveillance society. Chicago, IL: University of Chicago Press.

McCarty, M. (2014). Drug testing and crime-related restrictions in TANF, SNAP, and housing assistance. Congressional Research Service.

Office of the Assistant Secretary for Policy and Evaluation. (2011) Drug testing welfare recipients: Recent proposals and continuing controversies. U.S. Department of Health & Human Services.

Smith, V. (2013). Sociology of work : An encyclopedia. Thousand Oaks, California: SAGE Publications, Inc.

Walker, M.J. (2018). An argument against drug testing welfare recipients. Kennedy Institute of Ethics Journal, 28.

13. Encryption

Abbie Manse

Encryption, the encoding of data, is used to protect the privacy of information. Encryption is “a mapping of plaintext to ciphertext based on some chosen key text. It is performed by a stepwise application of a (more or less formalized) encryption algorithm” (Bauer, 2011, p. 416). Encryption works by scrambling text in a certain way so that only the recipient with the correct code can decipher the message. It is another step to try and conceal data from companies, individuals, or the government. Encryption is more simply defined as “the process of encoding data in such a way to render unusable to anyone except those in possession of the knowledge required to decrypt that data again” (Aitchison & Mechanic, 2009, p. 122). These definitions clarify the use and practicality of encryption.

With the use of encryption, online users can feel like they can protect personal information. Encryption allows people to take “some intriguing techno-precautions to manage their lives online… [such as encrypting] your emails and [forcing] recipients to use cryptographic keys to read them” (Gilliom & Monahan, 2013, p.70). Encryption allows people to have more control over what information is being sold and shared. Skype’s recent software update is an example of a company implementing encryption. Newman (2018) explains that “Skype will… implement the encryption, which is set up so that only the devices sending and receiving communications in a conversation can hear or view them” (p. 1). Users will be able to chat without the fear of their that someone is recording their data. By scrambling consumers’ conversations, encryption takes their privacy one step further and Skype is announcing to the world that they value their customers’ privacy.

References

Aitchison, A., & Machanic, A. (2009). Encryption. In Jonathan Gennick (Ed.), Expert SQL server 2008 development (pp. 121-158). New York, NY: Apress.

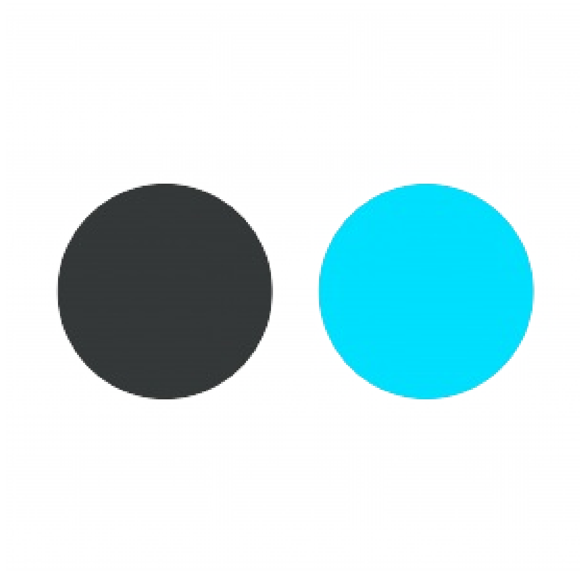
Bauer, F. L. (2011). Encryption. In van Tilborg, H. & S. Jajodia (Eds.), Encyclopedia of cryptography and security (pp. 416-417). Boston, MA: Springer.

Gilliom, J., & Monahan, T. (2013). SuperVision: An introduction to the surveillance society. Chicago, IL: University of Chicago Press.

Newman, L.H. (2018, January 11) Skype finally starts rolling out end to end encryption. Wired. Retrieved from: https://www.wired.com/story/skype-end-to-end-encryption-voice-text/.

14. **Filter Bubbles**

Hayden Hubbs



Filter bubbles are realms of online communities where users are segregated based on data gathered about our beliefs, likes, and dislikes. Newton (2016) describes filter bubbles as “the idea that personalization tools from companies like Facebook and Google have isolated us from opposing viewpoints, leading conservatives and liberals to feel like they occupy separate realities” (para. 1). These bubbles provide a comfortable space where user’s beliefs are not challenged which in turn leads to an obvious bias of material users consume. Filter bubbles are directly related to surveillance studies because it is through the observation of users that platforms generate filters.

Companies create this trove of data through the collection of data from sources including, likes on social media, what a person is viewing on

YouTube, news sources visited, and similar topics searched on the internet. For example, El-Bermawy (2016) claims many millennials use Facebook as their main website for political news. However, “our Facebook feeds are personalized based on past clicks and likes behavior, so we mostly consume political content that are similar to our views” (para. 4). Filter bubbles affect our ability to see and understand different perspectives on a topic. The 2016 United States Presidential election is a recent example of filter bubbles. The political divide is extremely evident in our country today and social media platforms reinforced those partisan differences.

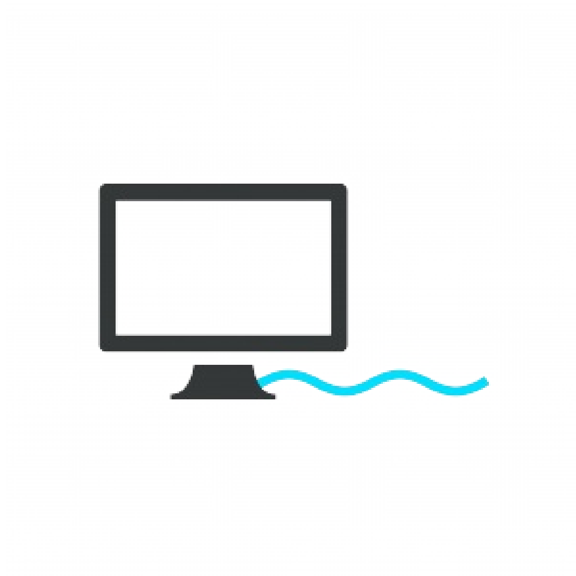
References

El-Bermawy, M. M. (2017, June 03). Your filter bubble is destroying democracy. Retrieved from https://www.wired.com/2016/11/filter-bubble-destroying-democracy/

Newton, C. (2016, November 16). The author of The Filter Bubble on how fake news is eroding trust in journalism. Retrieved from https://www.theverge.com/2016/11/16/13653026/filter-bubble-facebook-election-eli-pariser-interview

15. Internet Surveillance

Michelle Kurtz



Surveillance is defined as tracking or monitoring individuals with the purpose of changing their behavior (Gilliom & Monahan, 2012, p. 18). Internet surveillance is using tracking methods in order to alter behaviors. Since using the internet is an obligation in many places, it is an ideal platform to track and manipulate behavior. While people are in some way uncomfortable with their every move being tracked, they continue to use the internet anyway. Examples of internet surveillance include using Google Maps to get to a location, searching Google for restaurant recommendations, or YouTube tracking your views to suggest videos to watch. Internet surveillance is convenient and useful, fostering demand for surveilance-based features in online platforms.

A common method of tracking internet use is though cookies. Cookies are text files found in the memory of browsers that recognize devices as well as remember information (Gilliom & Monahan, 2013). These features that track online shopping and remember usernames and passwords. This convenient function can save people the time of having to manually sign in to a website they visit daily. Cookies also collect user activity, making the user's experience more convenient. However, these benefits are not free. Users provide information to advertisers that can be shared and analyzed. Advertisers collect massive amount of information through the internet. The data is used to build profiles of individuals to target them. It is often difficult to avoid sharing internet activity and information, which is why many people do not put extensive efforts into protecting their data Hill, 2012).

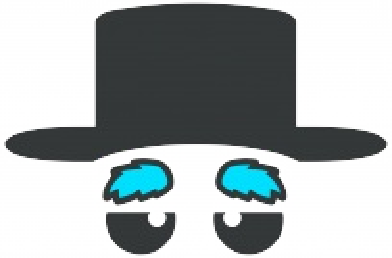
References

Gilliom, J., & Monahan, T. (2013). SuperVision: An introduction to the surveillance society. Chicago: University of Chicago Press.

Hill, K. (2012, March 1). Your digital self is on an auctioning block every single day. Forbes. Retrieved from https://www.forbes.com/sites/kashmirhill/2012/03/01/your-digital-self-is-on-an-auctioning-block-every-single-day/#51aac081782a

16. **Jeremy Bentham**

Ana Batley



Jeremy Bentham (1748-1832) was an English philosopher, social reformer, and lawyer. Throughout his life, he strived to become the "Newton of legislation," or provide humanity with structural social guidance the way Isaac Newton did with natural science (Everett, 1969). He was a social reformer with the convention of people being transparent and therefore accountable and responsible for their actions (Horne and Malay, 2014). He is known for popularizing Utilitarianism, or the philosophy of equality, abundance, subsistence, and security which connects to the Greatest Happiness Principle, that actions are morally correct if the majority of people benefit and are happy (Mack, 1969). It was by these principles that he would create all of his works.

In the 1780s, he invented an incredibly detailed plan for a building known as the Panopticon. His design was a circular building with a guard tower in the center, and the prisoners on the edges kept in isolation. The guards could see the prisoners, but the prisoners could not look at the guards, leaving them to act as though they were always being watched. Eventually, they would have disciplined themselves without the need for violence or multiple guards. This design was also intended for hospitals, factories, asylums, and schools. His plan never came to fruition due to changes of leadership in the British Parliament who were not fully committed to the plan (Horne and Malay, 2014).

Michael Foucault, a French philosopher, and historian, applied the method of prisoners reforming themselves due to the fear of being watched to surveillance in modern society. Instead of isolated prisoners, the general public is subject to surveillance from multiple angles such as phones and cameras. People are fearful that they are being watched, so they do not commit certain punishable acts. Bentham's idea of prisoners disciplining themselves was crucial in understanding the effects of surveillance in modern society through Foucault's theory (Horne and Malay, 2014).

Although Bentham never physically created the Panopticon, there are many recreations. For example, the Isla de la Juventud was a prison built in Cuba that could hold 2,500 prisoners. There were five circular towers and a central observation tower in the center of each. However, after the Cuban Revolution, the prison held over 8,000 prisoners causing overcrowding and an inability for the guards to see every person (Horne and Malay, 2014).

References

Dinwiddy, J. (1989). Bentham. New York, NY: Oxford City Press.

Everett, C. W. (1969). Jeremy Bentham. New York, NY: Dell

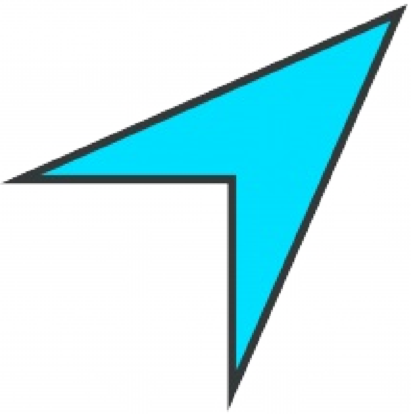
Publishing Co. Inc.

Horne, E. & Maly, T. (2014). The inspection house: An impertinent field guide to modern surveillance. Toronto, Canada: Coach House Books.

Mack, M. (Ed.). (1969). A Bentham Reader. New York, NY: Western Publishing Company.

17. **Location Data**

Ethan Roderick



Location Data is the accumulation of information regarding the whereabouts of an individual's, either in the past or present, by a service, organization, or network (Guide to Privacy). This data encompasses the knowledge of an individual's longitude, latitude, altitude, and direction of movement. In order to keep records of when an individual is in a specific place, an automatically updating and detailed time log is created by the user's habits. The knowledge of possibly being monitored can lead people to be, "constantly apprehensive and inhibited due to the constant presence of an unseen audience" (Sarpong and Rees, 2014, p. 217). The thought of always being tracked out of convenience, whether to find the nearest restaurant or for one's safety, has been subconsciously pushed to the back of user's minds as they don't make the connection between constant surveillance.

On smartphones, location data is developed and processed by one's phone carrier. However, these carrier's use contracts to distribute or sell this data to third-party organizations as well as bureaucratic organizations (Whitwam, 2018). The Information Commissioner's Office defines this location data as, "any data processed in an electronic communications network or by an electronic communications service indicating the geographical position of the terminal equipment of a user of a public electronic communications service" (Guide to Privacy). The phrase "any data" used here shows how even mundane and seemingly insignificant data, like taking a picture with a phone while having location services turned on, can be used for location pinpointing.

As more and more online functions and phone applications require location settings to be turned on, users begin to lose privacy. Whenever a person has his or her phone, their physical location is known and transmitted. Data leaks by the Strava app is an example the of the dangers of location services. Strava, which allows for detailed reports of running distances, shared aggregated user data on a worldwide public heat signature map. This map then revealed the locations of many secret military bases from runners using the apps on said bases. This was accomplished as, "the user data was released in November as a '2017 heatmap,' showing over 1 billion activities, including 13 trillion GPS datapoints" (Novak, 2018, para. 2). Therefore, as military men and women used this app and carried their phones during runs around their bases, their location data was able to be seen by users on the app which ultimately publicized their secret location.

References

Guide to privacy and electronic communications regulations. (n.d.). Information Commissioners Office. Retrieved from https://ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/location-data/

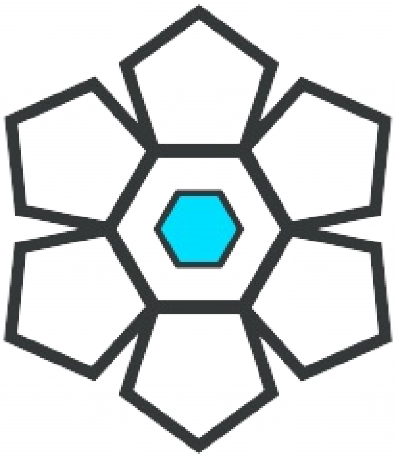
Novak, M. (2018, January 29). Fitness app's 'anonymized' data dump accidentally reveals military bases around the world. Gizmodo. Retrieved from https://gizmodo.com/fitness-apps-anonymized-data-dump-accidentally-reveals-1822506098

Sarpong, S., & Rees, D. (2014). Assessing the effects of 'big brother' in a workplace: The case of WAST. European Management Journal, 32(2), 216-222. doi:10.1016/j.emj.2013.06.008

Whitwam, R. (2018, May 15). Your cell carrier is selling your location data. Extreme Tech. Retrieved from https://www.extremetech.com/mobile/269259-your-cell-carrier-selling-your-location-data

18. **Millbank Prison**

Reagan Greene



Millbank Prison was a prison in Millbank, London, originally constructed as the National Penitentiary, which was used as a holding facility for prisoners before they were transported to Australia during most of the ninetieth century (Jackson, 2014). Architect and philosopher Jeremy Bentham originally bought the land for the project and planned to design the prison as a Panopticon. Bentham's project was later abandoned, Millbank was then designed by William Williams to reflect the Bentham's original work.

Millbank Prison is an important part of surveillance because it exemplifies the disciplinary society of the time and reflects upon architectural surveillance as a key factor in conformity. In the design, an inmate would not know whether they were being watched or not, they would have to assume they were under scrutiny at all times, leading to inmates to maintain their best behavior; thus order was assured by the presumption of constant surveillance, created by architecture and discipline (Lemon & Daniel, 2019). With a disciplinary society, control and continuous fear of castigation for their actions, kept the public in line and under governmental control; this also required "uniformity of outcome (be that education, military training, factory assembly, or healing) require a high personalized intervention)" (Horne & Malay, 2014, p. 23). This explains how the design of Millbank, octangular arrays that allow no personal privacy, in hopes of inspiring a change in character based upon the idea of constant surveillance. Horne and Malay also explain, "architecture serves to enhance these relationships, but its the surveillance that makes it all work" (Horne, 2014, p. 24).Meaning, that Millbank was in most regards, a revolutionary design that used surveillance to establish the idea of convicts correcting themselves in a disciplinary society

References

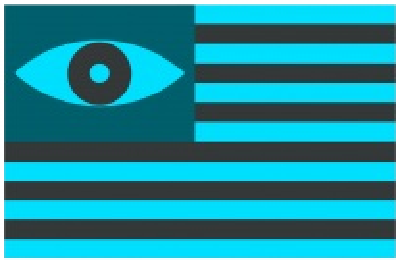
Jackson, A. (2014). Imprisonment and Millbank. Retrieved from https://www.digitalpanopticon.org/Imprisonment

Horne, E. & Maly, T. (2014). The inspection house: An impertinent field guide to modern surveillance. Toronto, Canada: Coach House Books.

Lemon, J. & Daniel, P. (2019). Millbank prison. Cholera and the Thames. Retrieved from https://www.choleraandthethames.co.uk/cholera-in-london/cholera-in-westminster/millbank-prison/

19. **National Security Agency**

Bella Foss



The National Security Agency (NSA), is a "U.S. intelligence agency within the Department of Defense that is responsible for cryptographic and communications intelligence and security" (National Security Agency, 2018, para. 1). The NSA's main function is to use surveillance to prevent attacks on, and promote the interests of, the United States of America. "The NSA grew out of the communications intelligence activities of U.S. military units during World War II. It was established in 1952 by a presidential directive from Harry S. Truman" (National Security Agency, 2018, para. 2). Harry S. Truman was nearing the end of his term when he created the NSA. One law that helps provide oversight for the NSA is the Freedom of Information Act (FOIA). "The Freedom Of Information Act (FOIA) generally provides that any person (with the exception of another federal agency, a fugitive from the law, or a representative of a foreign government) has a right, enforceable in court, to request access to federal agency records, except to the extent that such records (or portions thereof) are protected from disclosure by one of nine exemptions" (National Security Agency, 2005, para.2). This means that citizens can request information from the NSA.

Despite the ability of FOIA to provide oversight, the NSA's operations are controversial. "The National Security Agency, a component of the defense department, is engaged in unconstitutional surveillance of Americans' communications, including their telephone calls and emails. (Documents confirm, 2017, para. 1). Edward Snowden is famous for leaking classified NSA information and exposing agency abuses. "The Guardian publishes its first exclusive based on Snowden's leak, revealing a secret court order showing that the US government had forced the telecoms giant Verizon to hand over the phone records of millions of Americans" (Gidda, 2013, para. 3). The Snowden case is a prime example of how the NSA is surveilling US American citizens without their knowledge. Before Snowden's release of information citizens were unaware of the full extent of the surveillance they were to which they were subject.

References

Documents confirm how the NSA's surveillance procedures threaten Americans' privacy. (2017). American Civil Liberties Union. Retrieved from https://www.aclu.org/fact-sheet/documents-confirm-how-nsas-surveillance-procedures-threaten-americans-privacy

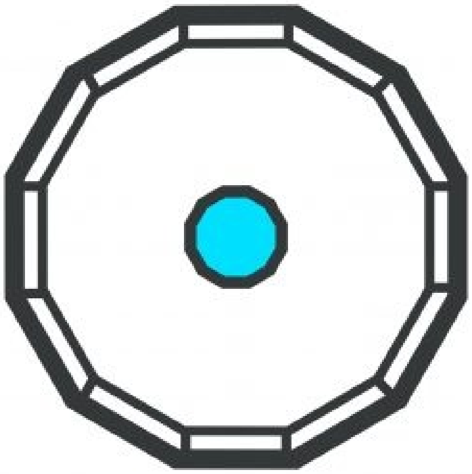
Gidda, M. (2013, August 21). Edward Snowden and the NSA files timeline. The Guardian. Retrieved from https://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline

Freedom of Information Act (2005). National Security Agency Retrieved from https://www.nsa.gov/Resources/Everyone/foia/

National Security Agency. (2018). Encyclopaedia Britannic. Retrieved from https://www.britannica.com/topic/National-Security-Agency

20. **Panopticon**

Nicholas Blake John



The Panopticon was created by architect Jeremy Bentham as an idea for a prison. It was a “peripheral building divided into cells for the inmates, which has a window facing out of the building and another facing the tower such that the backlighting effect would allow anyone within the tower to see all inmates” (Caluya, 2010, p. 622). It was then used by Michel Foucault, a philosopher, when he used the Panopticon as a model for surveillance in society. For Foucault, the Panopticon was the “the pinnacle of what he called the disciplinary society” (Horne and Maly, 2014, p. 18). This idea was constructed in a way that people would understand that they were always being surveyed by a disciplinary society, and therefore would not cause trouble and become docile due to the fear of being punished. For Foucault, the Panopticon is “instrument for enforcing discipline and punishment and a means of defining power relations in everyday lives” (Dobson and Fisher, 2013, p. 308). Having knowledge over a certain individual or group of people means that you can exercise power over those people.

An example of Panopticon is when, “individuals voluntarily enter into employment contracts and are therefore under an obligation to do during their working time as their employer demands. Employers have a corresponding right to check on their employees during work time or as long as employees are using their employers’ property” (Sthal, 2008). Since employees know that they can and are being surveilled while on the job, they need to be docile and constantly work so that they do not suffer any consequences.

References

Caluya, G. (2010). The post-panoptic society? Reassessing Foucault in surveillance studies. Social Identities, 16(5), 621–633. https://doi.org/10.1080/13504630.2010.509565

Dobson, J. E., & Fisher, P. F. (2007). The panopticon’s changing geography. Geographical Review, 97(3), 307–323. doi: 10.1111/j.1931-0846.2007.tb00508.x

Horne, E., & Maly, T. (2014). The inspection house: An impertinent field guide to modern surveillance. Toronto: Coach House Books.

Stahl, B. C. (2008). Forensic computing in the workplace: Hegemony, ideology, and the perfect panopticon? Journal of Workplace Rights, 13(2), 167–183. https://doi.org/10.2190/WR.13.2.e

21. Reasonable Suspicion

Connor Hock

Reasonable suspicion refers to the legal standard of proof that requires an objectively reasonable basis for suspecting criminal activity. A law enforcement officer must meet the reasonable suspicion standard to legally detain an individual or monitor their activity and behavior (Terry v. Ohio, 1968). In recent years, the United States Government has emphasized collecting criminal intelligence information through various surveillance methods. This approach raises concerns about policies and standards that may allow the invasion of one's privacy during surveillance. Under federal law, the government is only permitted to collect criminal intelligence information on someone if there is, "reasonable suspicion that the person has committed, is committing, or is about to commit a crime" (Terry v. Ohio, para.1).

The concept of reasonable suspicion can be frustrating to individuals because it is difficult to define, as it is often dependent on context and can be subjectively interpreted. This can be concerning to individuals because it creates the idea that the government can legally monitor them and invade their privacy due to relatively lax standards. In many situations, however, reasonable suspicion no longer meets the standard required to perform electronic surveillance on individuals suspected of committing a crime, due to legislation passed in recent years (Strasser, 2017). Most forms of electronic surveillance such as wiretapping or the use of a GPS tracker, now require a court-ordered warrant as they are considered to be a "search" under the Fourth Amendment (United States v. Jones, 2012).

There are still many circumstances however, in which reasonable suspicion is a sufficient standard for conducting surveillance. For example, if a police officer, responding to a call, noticed a car driving quickly away as he approached the crime scene, the officer could find that suspicious. Although the officer did not technically see the driver of the car commit a crime, the fact that the driver was fleeing the scene would constitute reasonable suspicion. Since the officer has now fulfilled the requirements of reasonable suspicion, he would be legally permitted to follow and further investigate the driver.

References

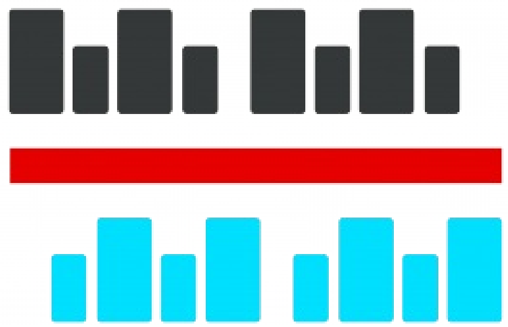
Terry v. Ohio, 392 U.S. 1 (1968).

Strasser, R. (2017, July 16). Electronic Surveillance. Retrieved October 24, 2018, from https://www.law.cornell.edu/wex/electronic_surveillance

United States v. Jones (2012), 565 US 400

22. Redlining

Anthony Ceja



Redlining is a practice of surveillance that is considered unethical and puts services such as loans and healthcare out of the grasp of residents of areas that were deemed low quality based on race or ethnicity. Redlining has been used in many large cities, to create divisions based on the communities and the type of people living in various sections of the city (Gaspaire). This concept connects to surveillance because redlined areas often have more police surveillance and fewer governmental services.

An example redlining would is the historic lending practices in Omaha, NE. Omaha's historic redlining map shows how the city was divided into sections rated A-D, with A being the more favorable parts of the city, and D being the least favorable. The areas sectioned off as D were the only palces where minority populations were allowed to live (Fletcher, 2017).

Though redlining is now illegal, its impact over decades is so strong that Omaha (and many other redlined cities) remain extremely segregated.

References

Fletcher, A. (2017). A history of redlining in Omaha. North Omaha history. Retrieved from https://northomahahistory.com/2015/08/02/a-history-of-red-lining-in-north-omaha/

Gaspaire, B. (n.d.). Redlining. Black past: Remembered and reclaimed. Retrieved from https://blackpast.org/aah/redlining-1937

23. **Stop and Frisk**

Nathan Barry

Stop and Frisk is defined as the brief, non-intrusive, warrantless stop by police of a suspect who the officer believes the suspect is armed and dangerous (Busby, 2017). These stops are also referred to as Terry stops due to the 1968 Supreme Court Case of Terry V. Ohio. However, in practice, these stops are seldom ever brief or non-intrusive. For example, the state of New York unfairly targeted young black males with their Stop & Frisk program (New York Civil Liberties Union, 2018). There has been much debate between civil rights activists and police organizations regarding when a Stop and Frisk search becomes a violation of our Fourth Amendment protections against unreasonable searches. This debate can be seen in the differing opinions of the Supreme Court cases of Rodriguez V. United States and Utah V. Strieff. Rodriguez V. Unites States determined that a drug sniffing dog being used for the purposes of a Terry stop was unconstitutional (Harvard Law Review, 2017). Utah V. Strieff, however, determined that evidence obtained via a Terry stop coupled with the discovery of an untainted warrant allowed the evidence discovered to be admissible in court (Harvard Law Review, 2015).

The use of Stop and Frisk by the New York Police Department has been a controversial practice since its inception in 2002. The New York Civil Liberties Union has gathered data regarding these stops since 2002 and every year, 80-90% of all stops target Blacks or Latinos between the ages of 14-24 with over 70% being innocent every year (New York Civil Liberties Union, 2018). When this power is abused by officers citizens face unconstitutional surveillance. Supporters of the program, including President Donald Trump, tout the programs propensity to decrease crime and claim that the unbalanced percentage of minorities being stopped accurately reflects the cities crime statistics (Madhani, 2018). Critics of the system claim that it has both failed to reduce crime, and that it gives officers too much flexibility in their searches with the low standard of reasonable suspicion (New York Civil Liberties Union, 2018).

References

Busby, J. C. (2017, December 24). Stop and frisk. Wex. Retrieved from https://www.law.cornell.edu/wex/stop_and_frisk

Madhani, A. (2018, October 08). Trump suggests Chicago police bring back controversial stop-and-frisk searches. USA Today. Retrieved from https://www.usatoday.com/story/news/2018/10/08/trump-chicago-stop-and-frisk-stem-gun-violence/1570409002/

Stop-and-frisk data. (2018, July 25). NYCLU. Retrieved from https://www.nyclu.org/en/stop-and-frisk-data

Utah v. Strieff. (2015). Harvard Law Review. Retrieved from https://harvardlawreview.org/2016/11/utah-v-strieff/

24. **Taylorism**

Annie Wheeler

Taylorism is the science of dividing specific tasks to allow employees to complete assignments as efficiently as possible. The practice of Taylorism was first developed by Frederick Taylor who desired to obtain the most efficient practices in the workforce. Seeking to eliminate soldiering, or the deliberation to slow a task for difficulty purposes, Taylor used scientific methods to assign workers to tasks they performed best(Gilliom and Monahan, 2013). According to Lanz (2013) “Division of labor has been an important source of productivity gains since the first human beings engaged in hunting and gathering” (p. 194). Taylor sought to attain a higher level of economic prosperity by his methods of division.

Surveillance techniques like Taylorism are used in large corporations to observe workers and make sure employees are not wasting company time by slacking in their tasks. By viewing the efficiency levels of each employee, companies can achieve the optimal success rate. Observation improves the dedication of employees to their work. Taylorism connects to the surveillance culture because employees are constantly under the pressure of being watched. Surveillance in the workplace can begin the second an employee drives into the parking lot. Gilliom and Monahan (2013) state, "Currently about 75 percent of employees at American companies are subjected to regular surveillance at the workplace, while employees who use the Internet at work stand a 33 percent chance of being exposed to constant surveillance" (p.93). There are multiple avenues of surveillance from being surveilled in the parking lot, scanning into the building, and to being watched over the Internet. The around the clock surveillance or lack thereof influences how hard employees work and spend their time (Hartzband & Groopman, 2016). Taylorism fails to care about the dignity of the human being as surveillance has the potential to imply a state of distrust between employees and their employers. Employees who surveil can negatively affect trusting relationships between employers and employees. Additionally, surveillance in the work environment places emphasis on achieving success and often puts success over care. Employees are challenged to work harder under the awareness that they are being watched.

An example of Taylorism in the modern-day workplace is the practice of timing emergency departments in hospitals and determining the shortest possible amount of time to attend to a patient. Hartzband and Groopman (2016) state, "physicians' sense that the clock is always ticking, and patients are feeling the effect" (p. 107). Physicians in certain clinics are only allowed to attend to the needs of patients for a very short period of time (Hartzband & Groopman). In shortened periods of time, doctors lack the ability to make decisions that listen to patients' preferences. Benefits of scientific management in hospitals are that more patients can receive care, communication becomes more concise, and diagnoses occur more rapidly. There are also negative setbacks to scientific management such as improper diagnoses, and lack of empathy towards the patient to receive the care they need.

References

Gilliom, J., & Monahan, T. (2013). SuperVision: An introduction to the surveillance society. Chicago: University of Chicago Press.

Hartzband, P. & Groopman, J. (2016). Medical Taylorism. The New England Journal of Medicine, 374, 106-108. doi: 10.1056/NEJMp1512402

Lanz, R. (2013). Offshoring of tasks: Taylorism versus Toyotism. The World Economy, 36, 194-212. doi: 10.1111/twec.12024

25. Terms of Service

Patrick Twomey

When downloading an app, creating an online account, joining a rewards program, and doing countless other things online, one will often be asked to agree to terms of service, or terms and conditions. Terms of service are a set of guidelines and permissions to which you and the other party involved (often a website or app) are agreeing. Frequently, these terms of service will be multiple pages long, with small print and large words. It is not uncommon for a person to skim through it quickly or not even read them at all, many do not even know what they agree to. When studying surveillance, a common theme is power, and terms of service are vital for big companies like Facebook and Google gain power over users. By agreeing, the users are essentially signing a contract with the other party. These documents can grant access to your photos, contacts, allow a company to sell your data to other companies. In almost every case, you will not be able to use a new account, or app without first agreeing to their terms of service. But once a user accepts the terms of service they are giving power to the other party. Users rarely pay attention to these agreements. According to Naughton (2014), there was a study performed by f-secure (a Finnish computer science company) free Wi-Fi to anyone who accepted the terms of service. The trick was that the terms of service granted F-Secure rights to the persons first born child. Everyone that was offered Wi-Fi accepted the terms. F-Secure was obviously never going to take the people's children, they just wanted to show that we should be more careful before blindly hitting accept.

An example of terms of service making causing controversy occurred in 2012. Instagram changed their terms of service, informing their users of the following, "You agree that a business or other entity may pay us to display your username, likeness, photos without any compensation to you" (Pogue, 2013, p.35). Many users expressed outrage at the change. Many people make a living off of Instagram, so this was possibly detrimental to their careers. Luckily not everyone skimmed through the terms of service and attention was brought to the problem. In response, Instagram changed their policy back to what it had been originally.

References

Naughton, J. (2014, Dec 13). State surveillance is enabled by our own sloppy habits- Our willingness to accept outrageous terms and conditions allows the Security Services to do as they wish. The Observer. Retrieved from https://infoweb.newsbank.com/resources/doc/nb/news/15250CC0AC p=AWNB

Pogue, D. (2013). Term of confusion. Scientific American, 308(3),

35.

26. **Terry Stops**

Josh Cantu

The 1968 Terry v. Ohio case established the legality of the Terry Stop, which is commonly known as the “stop and frisk.” The Terry Stop allows a police officer to stop someone and search them for weapons. Terry, the defendant in the case, was stopped and searched for weapons by a police officer because the officer thought that Terry was acting suspiciously. During the search, the officer found a gun (Terry v. Ohio). This is a type of surveillance because any pedestrian can be stopped and searched by a police officer if they are deemed to be “suspicious.”

The definition of “suspicious” is not always clear in Terry Stops. Often, law enforcement officers are left in the dark about what constitutes suspicious activity. One New York officer complained, “We are trained how to make stops, not when to make them” (Fagan & Geller, 2015, p.

57). When there is no real, set in stone definition of “suspicious,” a lot is left up to the judgment of the officer. What he sees as trying to prevent crime and keep the public safe, an onlooker can interpret as racist and malicious. In a study of the New York City Police Department (Gelman, Fagan, & Kiss, 2007) fopund, “blacks were stopped 23% more often than whites and Hispanics were stopped 39% more often than whites” (p. 822). This disparity supports arguments about racial bias in Terry Stops. The Terry Stop is likely to remain controversial due it’s lack of definition of “suspicion.”

References

Fagan, J., & Geller, A. (2015). Following the script: Narratives of suspicion in Terry Stops in street policing. University of Chicago Law Review 82(1), 51-88.

Gelman, A., Fagan, J., & Kiss, A. (2007). An analysis of the New York City Police Department’s “Stop-and-Frisk” policy in the context of claims of racial bias. Journal of the American Statistical Association, 102(479), 813-823. doi:10.1198/016214506000001040

Terry v. Ohio. (1968). Retrieved from: https://caselaw.findlaw.com/us-supreme-court/392/1.html